PAT-NO: JP02000251397A

DOCUMENT-IDENTIFIER: JP 2000251397 A

TITLE: METHOD AND SYSTEM FOR PROTECTING OPTICALLY RECOGNIZABLE

DATA ON DATA STORAGE

PUBN-DATE: September 14, 2000

INVENTOR-INFORMATION:

NAME	COUNTRY
PAUL, ROBERT HABERLE	N/A
GEORGE, KOKKOSURISU	N/A
STEPHEN, JOSEPH SUMORUSUKI	N/A

ASSIGNEE-INFORMATION:

NAME	COUNTRY
INTERNATL BUSINESS MACH CORP <IBM>	N/A

APPL-NO: JP2000045655

APPL-DATE: February 23, 2000

INT-CL (IPC): G11B020/10, G06K019/08 , G11B019/04

ABSTRACT:

PROBLEM TO BE SOLVED: To safely access the optically recognizable data by inserting a data storage into a reader, deciding whether or not the register data are registered in an electronic storage attached to the data storage and reading the data integrated in the data storage in response to that the register data coincide with user identification information.

SOLUTION: A processor unit 12 gains the user identification data with an eye scan, voice recognition and fingerprint detection, etc., by using an organism measuring device 52, and stores them in one of the data storages of a hard disk device 48 and a smart card 70, etc. A microprocessor 30 compares the user identification data from the smart card 70 with the register data from the

electronic storage attached to a smart compact disk 46 being the data storage, and when they agree, starts to reproduce the optically recognizable data from the smart compact disk 46.

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2000－251397
（P2000－251397Ａ）
(43)公開日　平成12年９月14日(2000.9.14)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'（参考）
Ｇ１１Ｂ　20/10		Ｇ１１Ｂ　20/10	Ｈ	
Ｇ０６Ｋ　19/08		19/04	５２１	
Ｇ１１Ｂ　19/04	５２１		５４１	
	５４１	Ｇ０６Ｋ　19/00	－ Ｆ	

審査請求　有　請求項の数44　ＯＬ　（全 22 頁）

(21)出願番号　特願2000－45655(P2000－45655)

(22)出願日　平成12年２月23日(2000.2.23)

(31)優先権主張番号　０９／２５７２２７

(32)優先日　平成11年２月25日(1999.2.25)

(33)優先権主張国　米国（ＵＳ）

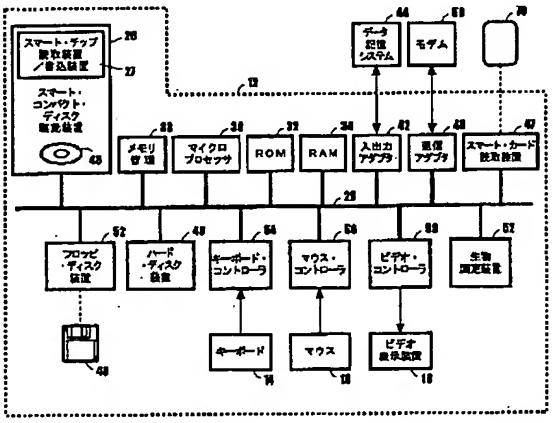
(71)出願人　390009531
インターナショナル・ビジネス・マシーンズ・コーポレーション
ＩＮＴＥＲＮＡＴＩＯＮＡＬ　ＢＵＳＩＮＥＳＳ　ＭＡＳＣＨＩＮＥＳ　ＣＯＲＰＯＲＡＴＩＯＮ
アメリカ合衆国10504、ニューヨーク州　アーモンク　（番地なし）

(74)代理人　100086243
弁理士　坂口　博　（外１名）

最終頁に続く

(54)【発明の名称】　データ記憶装置上の光学的に認識可能なデータを保護するための方法およびシステム

(57)【要約】
【課題】　データ記憶装置内に組み込まれた光学的に認識可能なデータへのアクセスを保護するための方法およびシステムを提供する。
【解決手段】　アクセスを保護するために、まず、データ記憶装置の読取装置への挿入に応答して、データ記憶装置に添付された電子記憶装置に登録データが記憶されているかどうかを判定する。その後、この登録データを、ユーザ識別データと比較する。その後、データ記憶装置上の光学的に認識可能なデータへのアクセスが、正しい識別によってのみ許可されるように、登録データとユーザ識別データの一致に応答して、データ記憶装置内に組み込まれた光学的に認識可能なデータが読み取られる。



【特許請求の範囲】
【請求項１】基板と、
前記基板が光学読取装置によって操作される時に読み取られるようになされた、前記基板内に組み込まれた光学的に認識可能なデータと、
２つの別個のセキュリティ分類のデータを同一のデータ記憶装置に記憶できるように、電子的に変更可能なデータを記憶するための、前記基板に取り付けられた電子記憶装置とを含む、データ記憶装置。
【請求項２】前記基板が、コンパクト・ディスクである、請求項１に記載のデータ記憶装置。
【請求項３】前記光学読取装置が、コンパクト・ディスク読取装置である、請求項１に記載のデータ記憶装置。
【請求項４】前記電子記憶装置が、スマート・チップである、請求項１に記載のデータ記憶装置。
【請求項５】さらに、
前記基板に取り付けられた、前記電子記憶装置に対する加重バランスを含む、請求項１に記載のデータ記憶装置。
【請求項６】データ記憶装置内に組み込まれた光学的に認識可能なデータへのアクセスを保護する方法であって、
データ記憶装置が読取装置に挿入されることに応答して、前記データ記憶装置に添付された電子記憶装置に登録データが記憶されているかどうかを判定するステップと、
前記登録データをユーザ識別データと比較するステップと、
データ記憶装置上の光学的に認識可能なデータへのアクセスが、正しい識別によってのみ許可されるように、前記登録データが前記ユーザ識別データと一致することに応答して、前記データ記憶装置内に組み込まれた前記光学的に認識可能なデータを読み取るステップとを含む方法。
【請求項７】さらに、
前記データ記憶装置上の前記光学的に認識可能なデータに対して行われるアクセスの数を追跡するために、前記光学的に認識可能なデータがアクセスされる時に、前記電子記憶装置に記憶された登録データを更新するステップを含む、請求項６に記載のデータ記憶装置に記憶された光学的に認識可能なデータへのアクセスを保護する方法。
【請求項８】さらに、
前記光学的に認識可能なデータへの定義済みの量のアクセスが行われた後に、前記光学的に認識可能なデータへのアクセスを制限するステップを含む、請求項７に記載のデータ記憶装置に記憶された光学的に認識可能なデータへのアクセスを保護する方法。
【請求項９】さらに、
前記データ記憶装置に添付された前記電子記憶装置に登録データが記憶されていない場合に、前記電子記憶装置に登録データを記憶するステップを含む、請求項６に記載のデータ記憶装置に記憶された光学的に認識可能なデータへのアクセスを保護する方法。
【請求項１０】前記データ記憶装置に添付された前記電子記憶装置に登録データが記憶されていない場合に、前記電子記憶装置に登録データを記憶する前記ステップが、さらに、
前記ユーザ識別データにアクセスするステップと、
前記電子記憶装置での記憶のための登録データとして前記ユーザ識別データを使用するステップとを含む、請求項９に記載のデータ記憶装置に記憶された光学的に認識可能なデータへのアクセスを保護する方法。
【請求項１１】前記ユーザ識別データにアクセスする前記ステップが、さらに、
スマート・カードを検出するステップと、
前記スマート・カードからの前記ユーザ識別データにアクセスするステップとを含む、請求項１０に記載のデータ記憶装置に記憶された光学的に認識可能なデータへのアクセスを保護する方法。
【請求項１２】前記データ記憶装置に添付された前記電子記憶装置に登録データが記憶されていない場合に、前記電子記憶装置に登録データを記憶する前記ステップが、さらに、
前記ユーザ識別データ内に含まれる特定の地理的地域を、前記電子記憶装置に記憶された所定の地理的地域と比較するステップと、
前記ユーザ識別データに含まれる前記特定の地理的地域が、前記電子記憶装置に記憶された前記所定の地理的地域と一致することに応答して、前記電子記憶装置での登録データの記憶を許可するステップとを含む、請求項９に記載のデータ記憶装置に記憶された光学的に認識可能なデータへのアクセスを保護する方法。
【請求項１３】前記登録データをユーザ識別データと比較する前記ステップが、さらに、
前記ユーザ識別データにアクセスするステップを含む、請求項６に記載のデータ記憶装置に記憶された光学的に認識可能なデータへのアクセスを保護する方法。
【請求項１４】前記ユーザ識別データにアクセスする前記ステップが、さらに、
スマート・カードを検出するステップと、
前記スマート・カードからの前記ユーザ識別データにアクセスするステップとを含む、請求項１３に記載のデータ記憶装置に記憶された光学的に認識可能なデータへのアクセスを保護する方法。
【請求項１５】前記ユーザ識別データにアクセスする前記ステップが、さらに、
前記読取装置に関連する、前記ユーザ識別データを記憶するスマート・チップを検出するステップと、
前記検出されたスマート・チップから前記ユーザ識別デ

ータを読み取るステップとを含む、請求項１３に記載のデータ記憶装置に記憶された光学的に認識可能なデータへのアクセスを保護する方法。
【請求項１６】前記ユーザ識別データにアクセスする前記ステップが、さらに、
前記読取装置を制御するオペレーティング・システムのインストール中に収集されたユーザ・データから前記ユーザ識別データを得るステップを含む、請求項１３に記載のデータ記憶装置に記憶された光学的に認識可能なデータへのアクセスを保護する方法。
【請求項１７】さらに、前記電子記憶装置上の前記登録データを変更するステップを含む、請求項６に記載のデータ記憶装置に記憶された光学的に認識可能なデータへのアクセスを保護する方法。
【請求項１８】前記電子記憶装置上の前記登録データを変更する前記ステップが、さらに、
前記光学的に認識可能なデータのすべてのコピーをアンインストールするステップと、
前記電子記憶装置から前記登録データを消去するステップとを含む、請求項１７に記載のデータ記憶装置に記憶された光学的に認識可能なデータへのアクセスを保護する方法。
【請求項１９】データ記憶装置内に組み込まれた光学的に認識可能なデータへのアクセスを保護するためのシステムであって、
データ記憶装置が読取装置に挿入されることに応答して、前記データ記憶装置に添付された電子記憶装置に登録データが記憶されているかどうかを判定するための手段と、
前記登録データをユーザ識別データと比較するための手段と、
データ記憶装置上の光学的に認識可能なデータへのアクセスが、正しい識別によってのみ許可されるように、前記登録データが前記ユーザ識別データと一致することに応答して、前記データ記憶装置内に組み込まれた前記光学的に認識可能なデータを読み取るための手段とを含むシステム。
【請求項２０】さらに、
前記データ記憶装置上の前記光学的に認識可能なデータに対して行われるアクセスの数を追跡するために、前記光学的に認識可能なデータがアクセスされる時に、前記電子記憶装置に記憶された登録データを更新するための手段を含む、請求項１９に記載のデータ記憶装置に記憶された光学的に認識可能なデータへのアクセスを保護するためのシステム。
【請求項２１】さらに、
前記光学的に認識可能なデータへの定義済みの量のアクセスが行われた後に、前記光学的に認識可能なデータへのアクセスを制限するための手段を含む、請求項２０に記載のデータ記憶装置に記憶された光学的に認識可能なデータへのアクセスを保護するためのシステム。
【請求項２２】さらに、
前記データ記憶装置に添付された前記電子記憶装置に登録データが記憶されていない場合に、前記電子記憶装置に登録データを記憶するための手段を含む、請求項１９に記載のデータ記憶装置に記憶された光学的に認識可能なデータへのアクセスを保護するためのシステム。
【請求項２３】前記データ記憶装置に添付された前記電子記憶装置に登録データが記憶されていない場合に、前記電子記憶装置に登録データを記憶するための前記手段が、さらに、
前記ユーザ識別データにアクセスするための手段と、
前記電子記憶装置での記憶のための登録データとして前記ユーザ識別データを使用するための手段とを含む、請求項２２に記載のデータ記憶装置に記憶された光学的に認識可能なデータへのアクセスを保護するためのシステム。
【請求項２４】前記ユーザ識別データにアクセスするための前記手段が、さらに、
スマート・カードからの前記ユーザ識別データにアクセスするためのスマート・カード読取装置を含む、請求項２３に記載のデータ記憶装置に記憶された光学的に認識可能なデータへのアクセスを保護するためのシステム。
【請求項２５】前記データ記憶装置に添付された前記電子記憶装置に登録データが記憶されていない場合に、前記電子記憶装置に登録データを記憶するための前記手段が、さらに、
前記ユーザ識別データ内に含まれる特定の地理的地域を、前記電子記憶装置に記憶された所定の地理的地域と比較するための手段と、
前記ユーザ識別データ内に含まれる前記特定の地理的地域が、前記電子記憶装置に記憶された前記所定の地理的地域と一致することに応答して、前記電子記憶装置での前記登録データの記憶を許可するための手段とを含む、請求項２２に記載のデータ記憶装置に記憶された光学的に認識可能なデータへのアクセスを保護するためのシステム。
【請求項２６】前記登録データをユーザ識別データと比較するための前記手段が、さらに、
前記ユーザ識別データにアクセスするための手段を含む、請求項１９に記載のデータ記憶装置に記憶された光学的に認識可能なデータへのアクセスを保護するためのシステム。
【請求項２７】前記ユーザ識別データにアクセスする前記手段が、さらに、
スマート・カードからの前記ユーザ識別データにアクセスするためのスマート・カード読取装置を含む、請求項２６に記載のデータ記憶装置に記憶された光学的に認識可能なデータへのアクセスを保護するためのシステム。
【請求項２８】前記ユーザ識別データにアクセスするた

めの前記手段が、さらに、
前記読取装置に関連する、前記ユーザ識別データを記憶するスマート・チップを検出するための手段と、
前記検出されたスマート・チップから前記ユーザ識別データを読み取るための手段とを含む、請求項２６に記載のデータ記憶装置に記憶された光学的に認識可能なデータへのアクセスを保護するためのシステム。
【請求項２９】前記ユーザ識別データにアクセスするための前記手段が、さらに、
前記読取装置を制御するオペレーティング・システムのインストール中に収集されたユーザ・データから前記ユーザ識別データを得るための手段を含む、請求項２６に記載のデータ記憶装置に記憶された光学的に認識可能なデータへのアクセスを保護するためのシステム。
【請求項３０】さらに、
前記電子記憶装置上の前記登録データを変更するための手段を含む、請求項１９に記載のデータ記憶装置に記憶された光学的に認識可能なデータへのアクセスを保護するためのシステム。
【請求項３１】前記電子記憶装置上の前記登録データを変更するための前記手段が、さらに、
前記光学的に認識可能なデータのすべてのコピーをアンインストールするための手段と、
前記電子記憶装置から前記登録データを消去するための手段とを含む、請求項３０に記載のデータ記憶装置に記憶された光学的に認識可能なデータへのアクセスを保護するためのシステム。
【請求項３２】データ記憶装置に組み込まれた光学的に認識可能なデータへのアクセスを保護するためのプログラム製品であって、
データ処理システム使用可能媒体と、
前記データ処理システム使用可能媒体を用いて符号化されたデータ記憶装置制御プログラムとを含み、前記データ記憶装置制御プログラムが、コンパクト・ディスク駆動装置へのコンパクト・ディスクの挿入に応答して、
データ記憶装置に添付された電子記憶装置に登録データが記憶されているかどうかを判定し、
前記登録データをユーザ識別データと比較し、
データ記憶装置上の光学的に認識可能なデータへのアクセスが、正しい識別によってのみ許可されるように、前記登録データが前記ユーザ識別データと一致することに応答して、前記データ記憶装置内に組み込まれた前記光学的に認識可能なデータを読み取るプログラム製品。
【請求項３３】前記データ記憶装置制御プログラムが、前記データ記憶装置上の前記光学的に認識可能なデータに対して行われるアクセスの数を追跡するために、前記光学的に認識可能なデータがアクセスされる時に、前記電子記憶装置に記憶された登録データを更新する、請求項３２に記載のプログラム製品。
【請求項３４】前記データ記憶装置制御プログラムが、前記光学的に認識可能なデータへの定義済みの量のアクセスが行われた後に、前記光学的に認識可能なデータへのアクセスを制限する、請求項３３に記載のプログラム製品。
【請求項３５】前記データ記憶装置制御プログラムが、前記データ記憶装置に添付された前記電子記憶装置に登録データが記憶されていない場合に、前記電子記憶装置に登録データを記憶する、請求項３２に記載のプログラム製品。
【請求項３６】前記データ記憶装置制御プログラムが、前記ユーザ識別データにアクセスし、前記電子記憶装置での記憶のための登録データとして前記ユーザ識別データを使用する、請求項３５に記載のプログラム製品。
【請求項３７】前記データ記憶装置制御プログラムが、スマート・カードからの前記ユーザ識別データにアクセスする、請求項３６に記載のプログラム製品。
【請求項３８】前記データ記憶装置制御プログラムが、前記ユーザ識別データ内に含まれる特定の地理的地域を、前記電子記憶装置に記憶された所定の地理的地域と比較し、前記ユーザ識別データに含まれる前記特定の地理的地域が、前記電子記憶装置に記憶された前記所定の地理的地域と一致することに応答して、前記電子記憶装置での登録データの記憶を許可する請求項３５に記載のプログラム製品。
【請求項３９】前記データ記憶装置制御プログラムが、前記ユーザ識別データにアクセスする、請求項３２に記載のプログラム製品。
【請求項４０】前記データ記憶装置制御プログラムが、スマート・カードからの前記ユーザ識別データにアクセスする、請求項３９に記載のプログラム製品。
【請求項４１】前記データ記憶装置制御プログラムが、前記読取装置に関連する、前記ユーザ識別データを記憶するスマート・チップを検出し、前記検出されたスマート・チップから前記ユーザ識別データを読み取る、請求項３９に記載のプログラム製品。
【請求項４２】前記データ記憶装置制御プログラムが、前記読取装置を制御するオペレーティング・システムのインストール中に収集されたユーザ・データから前記ユーザ識別データを得る、請求項３９に記載のプログラム製品。
【請求項４３】前記データ記憶装置制御プログラムが、前記電子記憶装置上の前記登録データを変更する、請求項３２に記載のプログラム製品。
【請求項４４】前記データ記憶装置制御プログラムが、前記光学的に認識可能なデータのすべてのコピーをアンインストールし、前記電子記憶装置から前記登録データを消去する、請求項４３に記載のプログラム製品。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、全般的にはデータ

・セキュリティのための方法およびシステムに関し、具体的には、データ記憶装置上の光学的に認識可能なデータへのアクセスを保護するための改良された方法およびシステムに関する。さらに具体的に言うと、本発明は、単一のデータ記憶装置上で2つの異なるセキュリティ・レベルのデータを記憶する方法およびシステムを提供する。

【0002】

【従来の技術】コンパクト・ディスクの急増に伴って、コンピュータ産業および一般家電産業の両方で、大量のデータを広く配布するための意味のある方法が確立された。現在入手可能な種類のコンパクト・ディスク（CD）には、オーディオCD（CD-DA）、データCD（CD-ROM）およびビデオCD（DVD）の3つが含まれる。CD-ROMでは、大量のデータは、アプリケーション・プログラム、オペレーティング・システムおよび、通常はコンピュータによって使用される一般的な情報を表すことができる。CD-DAとDVDには、通常は、ステレオまたはビデオ表示装置と共に使用するためのコンパクト・ディスク・プレーヤおよびDVDプレーヤなどの民生用機器による提示のために設計されたオーディオ・ビジュアル情報が含まれる。CD-ROM駆動装置およびDVD駆動装置も、コンピュータ内に含まれる可能性がある。

【0003】コンパクト・ディスクおよび他の光記憶媒体におけるデータの安全を確保しつつ配布することは、特にコンピュータ所有者がコンパクト・ディスクにデータをコピーできるようにする書き込み可能なコンパクト・ディスク駆動装置の発展に伴って、産業界で認められている問題である。コンパクト・ディスクによって配布される内容の著作権者は、自己の知的所有権を保護し、最初にコンパクト・ディスクに記憶された著作物たるデータの許可されない使用またはコピーを防ぐための解決策を探してきた。製造業者がCD-ROMデータを保護するために講じた処置については、CD-ROMに記憶されたデータにアクセスするためにユーザが入力しなければならない「ソフトウェア・キー」の使用がある。ソフトウェア・キーは、通常、CD-ROMの文書に含まれるか、CD-ROMのカバーに直接書き込まれる複数桁の数字である。そのようなソフトウェア・キーを使用しても、作成することのできるコンパクト・ディスク上のデータのコピーの数を制限することにはならず、コンパクト・ディスクの購入者が、データを他人がコピーできるようにすることを制限することにもならない。

【0004】DVDの場合、DVD内容の所有者がDVDタイトルを世界中で公開するので、地理的に異なる地域で配布の時期を制御する必要があることがしばしばである。地理的なタイミングの制御は、現在は、検出された時に特定の地域で配布される対応するDVDプレイヤでDVDを再生できるようにする、特殊な地域ビットを用いて各DVDを特別に符号化することによって達成される。しかし、この方法論は、特殊な地域ビットがプログラムされている特定の地域用のDVDプレイヤを取得することによって、簡単に迂回できる。

【0005】したがって、上で示した理由および他の多数の理由から、すべての種類のコンパクト・ディスク上のデータを保護する方法を実施し、コンパクト・ディスクの内容の所有者が、コンパクト・ディスクに記憶されたデータの使用を制御できるようにすることが望ましい。

【0006】

【発明が解決しようとする課題】したがって、本発明の目的は、データ・セキュリティのための方法およびシステムを提供することである。

【0007】本発明の他の目的は、データ記憶装置上の光学的に認識可能なデータへのアクセスを安全にするための改良されたシステムおよび方法を提供することである。

【0008】本発明のさらなる目的は、単一のデータ記憶装置上で2つの別個のセキュリティ分類のデータを記憶するためのシステムおよび方法を提供することである。

【0009】

【課題を解決するための手段】前述の目的は、これから説明する形で達成される。データ記憶装置内に組み込まれた光学的に認識可能なデータへのアクセスを安全にするための方法およびシステムを提供する。アクセスを安全にするために、まず、データ記憶装置を読取装置へ挿入すると、それに応じて、データ記憶装置に添付された電子記憶装置に登録データが記憶されているかどうかを判定する。次に、登録データを、ユーザ識別データと比較する。そして、登録データがユーザ識別データに一致することに応答して、データ記憶装置に組み込まれた光学的に認識可能なデータが読み取られ、データ記憶装置上の光学的に認識可能なデータへのアクセスが、正しい識別によってのみ許可されるようにする。

【0010】基板と、光学的に認識可能なデータおよび電子記憶装置とを含むデータ記憶装置を提供する。光学的に認識可能なデータは、基板内に組み込まれ、基板が光学読取装置によって操作される時に読み取られるようになされている。電子記憶装置は、基板に取り付けられ、電子的に変更可能なデータを記憶するのに使用され、2つの別個のセキュリティ分類のデータを同一のデータ記憶装置上で記憶できるようにする。

【0011】

【発明の実施の形態】ここで図面、具体的には図1を参照すると、そこにインストールされたオペレーティング・システムを使用するデータ処理システム10の代表的なハードウェア環境の図が示されている。データ処理システム10には、プロセッサ・ユニット12、キーボー

ド14、マウス16およびビデオ表示装置（またはモニタ）18が含まれる。キーボード14およびマウス16は、ユーザ入力装置を構成し、ビデオ表示装置18は、ユーザ出力装置を構成する。マウス16は、ビデオ表示装置18の画面22に表示されるカーソル20を制御するのに使用される。データ処理システム10は、グラフィカル・ユーザ・インターフェース（GUI）をサポートし、これによって、ユーザは、ユーザ・コマンドを実行するために、マウス16を介してカーソル20をアイコンまたは画面22上の特定の位置に移動し、マウス16のボタンのうちの1つを押し下げることによって、「ポイントアンドクリック」を行うことができる。フロッピ・ディスク駆動装置24、スマート・コンパクト・ディスク駆動装置26およびスマート・カード読取装置47は、プロセッサ・ユニット12に外部データ記憶装置へのアクセスを提供する。

【0012】ここで図2を参照すると、図1に示されたデータ処理システム10の機能ブロック図が示されている。プロセッサ・ユニット12には、システム・バス28が含まれ、システム・バス28にはさまざまな機能ブロックが接続され、システム・バス28によって、さまざまな機能ブロックの間の通信が達成される。システム・バス28に接続されたマイクロプロセッサ30は、読取専用メモリ（ROM）32およびランダム・アクセス・メモリ（RAM）34によってサポートされ、ROM32とRAM34の両方が、システム・バス28に接続される。

【0013】ROM32には、他のコードの中でも、ハード・ディスク装置36およびフロッピ・ディスク駆動装置24の相互作用など、ある基本的なハードウェア動作を制御する基本入出力システム（BIOS）または他のファームウェアが含まれる。RAM34は、主記憶であり、この主記憶内で、本発明を組み込まれたオペレーティング・システムおよび他のアプリケーション・プログラムが動作する。メモリ管理装置38は、RAM34と、ハード・ディスク装置36、フロッピ・ディスク駆動装置24またはスマート・コンパクト・ディスク駆動装置26との間のデータのページングなどの直接メモリ・アクセス（DMA）動作のすべてを制御するためにシステム・バス28に接続される。本発明の実施を指示するアプリケーション・プログラムは、データ処理システム10の記憶媒体への記憶のためにフロッピ・ディスク駆動装置24によって読取可能とすることができるさまざまな信号担持媒体を介して、ハード・ディスク装置36などの記憶媒体への記憶のためにデータ処理システム10に供給することができる。信号担持媒体は、フロッピ・ディスク40などの書込可能媒体を含むがこれに制限されない。アプリケーション・プログラムは、オペレーティング・システムによってサポートされるさまざまなプログラミング言語で記述することができる。プログラミング言語はC++を含むがこれに制限されない。

【0014】さらに図2を参照すると、データ記憶システム44などのデータ記憶周辺装置のためのインターフェースを提供するためにシステム・バス28に接続された入出力アダプタ42が示されている。データ処理システム10によってアクセス可能な記憶容量を拡張するために、追加の入出力アダプタを含めることができる。

【0015】用語「スマート・カード」は、当技術分野で周知の形で、以下の説明で時折使用される。さらに、用語「スマート・チップ」および「スマート・カード受入装置」も使用される。スマート・カードは、一般的に、特殊な空洞にマイクロモジュールを組み込まれた、プラスチックの本体から形成されるカードを指す。スマート・チップは、一般的に、スマート・カードに組み込まれたマイクロモジュールを指し、電子的に変更可能なデータを含む電子記憶装置が典型的である。スマート・カード受入装置は、スマート・カード内のスマート・チップからデータを読み取り、これにデータを書き込む。

【0016】スマート・カード受入装置47は、スマート・カード70を含む形で図示されており、スマート・カード受入装置47によって、マイクロプロセッサ30がスマート・カード70と通信できるようになる。スマート・カード受入装置47は、当技術分野で周知の通り、モデム50と共にまたは他のPCMCIAスロットに組み込むこともできる。さらに、スマート・チップは、スマート・カード受入装置47に追加してまたはこれの代わりにプロセッサ・ユニット12のハードウェアに組み込むことができる。さらに、スマート・カード受入装置47に類似の受入装置が、スマート・カード70に似た、カードのメモリ内のデータへのアクセスおよびタンパリングを防ぐためのセキュリティ機能を備えることが既知のセキュア・カードまたはPCMCIAカードも受け入れることができる。

【0017】当技術分野で新規のスマート・コンパクト・ディスク駆動装置26が、そこに挿入された、スマート・コンパクト・ディスク46などのデータ記憶装置を含む形で図示されている。CD-ROM、CD-DAおよびDVD上のデータにアクセスするためのコンパクト・ディスク駆動装置および他の光記憶媒体読取装置は、当技術分野で知られている。しかし、スマート・コンパクト・ディスク駆動装置26には、スマート・カード受入装置と同じ方法で、スマート・コンパクト・ディスク46に取り付けられた電子記憶装置やスマート・チップからデータを読み取ったり、これにデータを書き込んだりするスマート・チップ読取装置／書込装置27も含まれる。スマート・チップ読取装置／書込装置27は、電子記憶装置に記憶されたデータを電子的に変更することができる。

【0018】生物測定装置52を使用して、眼球スキャン、音声認識または指紋検出などの形でユーザ識別デー

タを提供することができる。このようなユーザ識別データは、ハード・ディスク装置３６およびスマート・カード７０を含む、プロセッサ・ユニット１２のデータ記憶装置のうちの1つに記憶することができる。ユーザ識別は、データ処理システム１０へのアクセスのためのパスワードとして使用することができる。

【００１９】光記憶媒体、プリンタなどの他の周辺装置も、データ処理システム１０に追加することができる。さらに、ゲーム・カートリッジ読取装置または他の電子媒体読取装置などの記憶媒体の他の読取装置を、データ処理システム１０に組み込むことができる。さらに、通信アダプタ４８を使用して、他のデータ処理システム（図示せず）と通信することができる。通信アダプタ４８は、モデム５０または、イーサネット・リンクなどのネットワーク・リンク（図示せず）をサポートすることができ、これによって、データ処理システム１０が、他のデータ処理システムと通信することができるようになる。モデム５０を用いると、データ処理システム１０が、公衆交換電話網（ＰＳＴＮ）回線またはＩＳＤＮ回線を含むがこれに制限されないデータ転送回線を介してインターネット上の他のデータ処理システムと通信できるようになる。モデム５０の他に、通信アダプタ４８は、ローカル・エリア・ネットワーク（ＬＡＮ）に接続されたネットワーク・リンクなどの他の通信装置をサポートすることができる。

【００２０】プロセッサ・ユニット１２の説明を完了するために、３つの入出力コントローラすなわち、キーボード・コントローラ５４、マウス・コントローラ５６およびビデオ・コントローラ５８があり、これらのすべてが、システム・バス２８に接続される。名前からわかるように、キーボード・コントローラ５４は、キーボード１４のためのハードウェア・インターフェースを提供し、マウス・コントローラ５６は、マウス１６のためのハードウェア・インターフェースを提供し、ビデオ・コントローラ５８は、ビデオ表示装置１８のためのハードウェア・インターフェースを提供する。図1および図2は、通常の汎用コンピュータを表すが、光学的に認識可能なデータ、具体的にはコンパクト・ディスクを含むデータ記憶装置に記憶されたデータへのアクセスを提供する、ビデオ表示システム、オーディオ・サウンド・システムおよび他のデータ処理システム内に組み込むこともできる。

【００２１】ここで図3を参照すると、本発明の方法およびシステムと共に使用することができるスマート・カードの高水準の図が示されている。スマート・カード７０には、スマート・チップ７２の接点が露出される形で標準的なスマート・チップ７２を中に組み込まれた、符号７１に示されたクレジット・カード大のプラスチック・エンケーシングが含まれる。スマート・チップ７２は、関連するメモリおよびメモリ制御論理と共に集積回路またはマイクロプロセッサを含む、静的電子記憶装置であることが好ましい。オペレーティング・システムは、スマート・チップ７２内に組み込まれる。電力が印加された時に、スマート・チップ７２は、初期設定され、動作を開始する。

【００２２】スマート・カード７０の寸法は、国際規格（ＩＳＯ　７８１６）によって定められている。ユーザがスマート・カード７０を正しい向きでスマート・カード読取装置に挿入できるようにするために、方向標識７５などの方向標識が、通常はスマート・カード７０の外面に指示されている。ＩＳＯ　７８１６規格では、温度範囲と柔軟性を含むプラスチックの物理的特性、電気接点の位置およびスマート・チップ７２がスマート・カード読取装置と通信する方法も定義されている。スマート・チップ７２は、約１３ｍｍ×１２ｍｍの大きさで、厚さは０．５ｍｍ未満である。

【００２３】スマート・カードは、ユーザ識別データ、電子財布およびクレジット・カードなどの応用分野のための携帯用データ記憶検索装置として国際規格になりつつある。スマート・カードは、通常は、スマート・カードを持つすべての人、スマート・カード保持者のみおよび第三者を含む3レベルのセキュリティ用に設計することができる。パスワードを必要としないスマート・カードは、そのスマート・カードを持っているすべての人が使用することができる。たとえば、患者の名前と血液型を含む医療スマート・カードは、パスワードなしでアクセス可能にすることができる。カード保持者スマート・カードは、ユーザ識別番号または他のパスワード・データが正しく入力された場合に限って使用することができる。たとえば、眼球スキャンのユーザ検証データをスマート・カードに含めることができ、この場合、スマート・カードに記憶されたデータにアクセスするためには、眼球スキャンがカードのユーザ検証データと一致しなければならない。最後に、第三者は、その第三者だけがデータにアクセスすることができるスマート・カードを発行することができる。たとえば、スマート・カードに電子財布が含まれる場合には、それを発行する銀行だけが、財布を再ロードすることができる。このようなスマート・カードには、スマート・カード保持者が電子財布を用いて購入を行えるようにするだけのためのパスワード検証方式も含めることができる。

【００２４】スマート・カードは、読取専用、追加専用、更新専用またはアクセス不能の情報を含むように設計することができる。スマート・カードに含まれる情報の種類を促進するために、複数の種類のメモリを含めることができる。たとえば、読取専用アクセス・メモリ（ＲＯＭ）に加えてスマート・カードに含めることができる４種類のメモリは、プログラマブルＲＯＭ（ＰＲＯＭ）、消去可能プログラマブルＲＯＭ（ＥＰＲＯＭ）、電気的消去可能ＰＲＯＭ（ＥＥＰＲＯＭ）およびランダ

ム・アクセス・メモリ（ＲＡＭ）である。

【００２５】図３を参照すると、スマート・チップ７２は、信号および電圧の入出力のために８つの接点を設けられることが好ましい。Ｖｃｃ信号は、符号７４に図示されており、Ｖｃｃは、スマート・チップ７２を駆動するためにスマート・チップ７２に供給され、通常は５Ｖである。ＧＮＤ信号は、符号８０に図示されており、Ｖｃｃ電位が測定される基準のグラウンドである。ＲＳＴ信号は、符号７６に示されており、ＲＳＴは、電力投入後にマイクロプロセッサの状態を初期設定するのに使用される信号線である。次に、ＣＬＫ信号が符号７８に示されており、ＣＬＫ信号は、スマート・チップ７２の論理回路を駆動するのに使用される。Ｖｐｐ信号は、符号８２に示されており、Ｖｐｐは、ＥＰＲＯＭメモリのプログラムおよびＶｃｃより高い電圧供給を必要とする他の事象に必要な、スマート・チップ７２に供給される高電圧供給信号である。次に、Ｉ／Ｏコネクタが符号８４に示されており、これは、スマート・チップ７２がデータおよびコマンドの送受に使用するシリアル入出力コネクタである。２つの信号パッド８６および８８は、現在は未定義である。

【００２６】次に図４を参照すると、本発明の方法およびシステムによるスマート・コンパクト・ディスク４６の絵図が示されている。スマート・コンパクト・ディスク４６は、寸法は標準コンパクト・ディスクであり、当技術分野で周知の形で機能する。スマート・コンパクト・ディスク４６には、光学的に認識可能なデータ記憶区域６０と非光学区域６２を有する基盤が含まれる。光学的に認識可能なデータ記憶区域６０は、光学的に認識可能なデータを組み込まれることが好ましい。スマート・コンパクト・ディスク４６には、少なくとも１つのスマート・チップ７２または他の電子記憶装置も含まれる。光学的に認識可能なデータ記憶区域６０およびスマート・チップ７２には、２つの明瞭に異なるセキュリティ分類のデータを格納することができる。また、図示の実施例では、２つのスマート・チップ７２および７３が含まれ、各スマート・チップは、スマート・コンパクト・ディスク４６が正しく回転するように、他のスマート・チップの重量のバランスをとるために配置される。しかし、他の実施例では、スマート・チップ７３の代替装置を、スマート・チップ７２の重量のバランスをとるためにスマート・チップ７２の反対側に配置することができる。

【００２７】ここで図５ないし図９を参照すると、本発明の方法を示す高水準論理流れ図が示されている。図５ないし図９は、所望の結果につながる、自己矛盾のないステップのシーケンスを表す。これらのステップは、物理量の物理的操作を必要とするステップである。必然的にというわけではないが、通常、これらの量は、記憶、転送、組合せ、比較および他の操作が可能な電気信号または磁気信号の形をとる。これらの信号を、ビット、値、要素、記号、文字、項、数または類似物と称することが、時として便利であることが、当業者によって証明されている。しかし、これらおよび類似の用語のすべてが、適当な物理量に関連し、その物理量に適用される単に便利なラベルであることに留意されたい。

【００２８】さらに、実行される操作は、用語として、加算または比較などと称することがしばしばである。そしてそれらの用語は、一般に人間の操作員によって実行される心理的操作に関連づけられる。人間の操作員のそのような能力は、ほとんどの場合に、本明細書に記載の動作のいずれにおいても必要でもなく望ましくもない。本発明に記載の動作は、本発明の一部を形成する。これらの動作は、機械動作である。本発明の好ましい実施例の動作を実行するのに有用な機械には、汎用ディジタル・コンピュータなどのデータ処理システム、ビデオ表示システム、オーディオ・サウンド・システムまたは他の類似の装置が含まれる。どの場合でも、方法動作とコンピュータの動作と計算自体の方法の間の区別に留意されたい。本発明は、電気信号または他の物理信号を処理して所望の物理信号を生成する際の、図２のプロセッサ・ユニット１２などのプロセッサ・ユニットを動作させるための方法ステップに関する。

【００２９】ここで図５を参照すると、前に登録されていない場合の、スマート・コンパクト・ディスク、具体的にはスマートＣＤ−ＲＯＭに取り付けられたスマート・チップへの登録データのインストールを示す高水準論理流れ図が示されている。さらに、この処理では、スマートＣＤ−ＲＯＭに記憶されたソフトウェアを所有者がインストールすることを許可することができる。図からわかるように、図５に示された処理は、ブロック９０で開始され、その後、ブロック９２に進む。マイクロプロセッサ３０の動作における複数のトリガが、ブロック９０で開始される処理のトリガになる可能性がある。たとえば、スマート・コンパクト・ディスクの検出時に、この処理にトリガをかけることができる。

【００３０】ブロック９２は、スマート・カードからのユーザ識別データの読取を示す。ユーザ識別データには、スマート・カード保持者の氏名、住所、電話番号を、所有権を識別するためにスマート・コンパクト・ディスクに記憶することのできる他のユーザ・データと共に含めることができる。この処理および下記の処理では、ユーザ識別データを含むスマート・チップを、データ処理システムにも組み込み、そこから、ユーザ識別データを読み取ることができる。さらに、コンパクト・ディスクに取り付けられたスマート・チップに記憶するためのユーザ識別データを収集するもう１つの方法は、データ処理システムのためのオペレーティング・システムのインストール中にデータ処理システムによって収集されたユーザ識別データを介する。必要であれば、スマー

ト・カードで典型的なとおり、ユーザ識別データに、パスワードによってまたは、生物測定装置５２などの生物測定装置から収集したデータによって、アクセスすることができる。

【００３１】ブロック９２の後に、処理はブロック９４に進む。ブロック９４は、スマート・コンパクト・ディスクに取り付けられたスマート・チップからの登録データの読取を示す。その後、処理はブロック９６に進む。ブロック９６は、登録データが、スマート・コンパクト・ディスクに取り付けられたスマート・チップに前にインストールされたかどうかの判定を示す。スマート・チップのための登録データをインストールする必要がある場合には、処理はブロック９８に進む。そうでなく、スマート・チップのための登録データが前にインストールされている場合には、処理はブロック１０６に進む。

【００３２】さらに図５を参照すると、ブロック９８は、登録データとして記憶するための、スマート・チップへのユーザ識別データのコピーを示す。ユーザ識別データは、スマート・コンパクト・ディスクに取り付けられたスマート・チップに転送され、スマート・チップに関連するメモリに記憶される。その後、処理はブロック９８からブロック１００に進む。ブロック１００は、インストール・カウンタを１つ減分することを示す。インストール・カウンタは、スマート・チップに関連する、ユーザによってアクセス可能でないメモリに記憶される。インストール・カウンタには、ユーザが行うことができる、スマート・コンパクト・ディスクに記憶されたソフトウェアのコピーの事前に設定された回数が含まれる。ブロック１００の後に、処理はブロック１０２に進む。ブロック１０２は、スマート・コンパクト・ディスクからデータ記憶装置へのソフトウェア・プログラムのインストールを示す。スマート・コンパクト・ディスクが正しく登録されているならば、このソフトウェアはアクセスのためにロックを解除される。その後、この処理はリターンする。

【００３３】さらに図５を参照すると、ブロック１０６は、スマート・カードからのユーザ識別データと、スマート・コンパクト・ディスクに取り付けられたスマート・チップからの登録データの比較を示す。その後、処理はブロック１０６からブロック１０８に進む。ブロック１０８は、ユーザ識別データが登録データと一致するか否かの判定を示す。ユーザ識別データが登録データと一致すると判定された場合には、処理はブロック１１０に進む。ユーザ識別データが登録データと一致しないと判定された場合には、処理はブロック１１２に進む。ブロック１１０は、インストール・カウンタが０に等しいか否かの判定を示す。インストール・カウンタが０に等しい場合には、スマート・コンパクト・ディスクが登録された所有者がソフトウェアの追加コピーを得ることはできず、処理はブロック１１２に進む。インストール・カウンタが０に等しくない場合には、処理はブロック１００に進む。ブロック１１２は、正しい識別が供給されなかったのでソフトウェアをインストールできない場合のエラー・メッセージの表示を示す。その後、処理はリターンする。

【００３４】次に図６を参照すると、本発明の方法およびシステムによる、スマート・コンパクト・ディスク、具体的にその中にソフトウェアを組み込まれたスマートＣＤ－ＲＯＭの所有権をアンインストールする方法の高水準論理流れ図が示されている。図からわかるように、図６に示された処理は、ブロック１２０で開始され、その後、ブロック１２２に進む。マイクロプロセッサ３０の動作における複数のトリガが、ブロック１２０で開始される処理のトリガになる可能性がある。たとえば、スマート・コンパクト・ディスクの所有権をアンインストールを求めるユーザ要求の検出時に、この処理にトリガをかけることができる。

【００３５】ブロック１２２は、スマート・カードからのユーザ識別データの読取を示す。ブロック１２２の後に、処理はブロック１２４に進む。ブロック１２４は、スマート・コンパクト・ディスクに取り付けられたスマート・チップからの登録データの読取を示す。その後、処理はブロック１２４からブロック１２６に進む。ブロック１２６は、スマート・コンパクト・ディスクに取り付けられたスマート・チップに前に登録データがインストールされたか否かの判定を示す。スマート・チップのための登録データをインストールする必要がある場合には、処理はブロック１２８に進む。ブロック１２８は、スマート・チップに前のソフトウェア・インストールの記録がないので、エラー・メッセージが表示されることを示す。ブロック１２６で、スマート・チップのための登録データが前にインストールされている場合には、処理はブロック１３０に進む。

【００３６】さらに図６を参照すると、ブロック１３０は、スマート・カードからのユーザ識別データと、スマート・コンパクト・ディスクに取り付けられたスマート・チップからの登録データの比較を示す。その後、処理はブロック１３０からブロック１３２に進む。ブロック１３２は、ユーザ識別データが登録データと一致するか否かの判定を示す。データが一致する場合には、処理はブロック１３４に進む。データが一致しない場合には、処理はブロック１４０に進む。ブロック１４０は、正しい識別が供給されなかったのでエラー・メッセージが表示されることを示す。

【００３７】さらに図６を参照すると、ブロック１３４は、インストール・カウンタを１つ増分することを示す。その後、処理はブロック１３４からブロック１３６に進む。ブロック１３６は、インストール・カウンタが最大値に達したか否かの判定を示す。コンパクト・ディスクに記憶されたデータから作ることのできる最大のコ

ピー数は、スマート・コンパクト・ディスク製造者によって事前に設定される。各コピーについて、コンパクト・ディスクを正しく登録するために登録データを記憶しなければならない。インストール・カウンタが最大値に達したと判定される場合には、処理はブロック１４２に進む。ブロック１４２は、スマート・チップからの登録データの消去を示す。その後、処理はブロック１３８に進む。ブロック１３８は、ソフトウェア・プログラムのアンインストールを示す。プログラムのアンインストール処理は、消費者が、ソフトウェアのコピーを残さずにソフトウェアを含むスマート・コンパクト・ディスクを別の個人に販売することができるようにするために含まれる。

【００３８】ここで図７を参照すると、本発明の方法およびシステムによる、スマート・コンパクト・ディスク上のオーディオ・データにアクセスするための、スマート・コンパクト・ディスク、具体的にはオーディオＣＤの登録のための処理の高水準論理流れ図が示されている。図からわかるように、図７の処理は、ブロック１０５で開始され、その後、ブロック１５２に進む。マイクロプロセッサ３０の動作における複数のトリガが、ブロック１５０で開始される処理のトリガになる可能性がある。たとえば、スマート・コンパクト・ディスクの検出時に、この処理にトリガをかけることができる。

【００３９】ブロック１５２は、スマート・カードからのユーザ識別データの読取を示す。前に説明したように、ユーザ識別データは、ハードウェアに組み込まれたスマート・チップなどの他の供給源から、または、オペレーティング・システムのインストール中に収集されたユーザ識別データから、得ることもできる。ブロック１５２の後に、処理はブロック１５４に進む。ブロック１５４は、スマート・コンパクト・ディスクに取り付けられたスマート・チップからの登録データの読取を示す。その後、処理はブロック１５６に進む。ブロック１５６は、スマート・コンパクト・ディスクに取り付けられたスマート・チップに登録データが前にインストールされたか否かの判定を示す。スマート・チップのための登録データをインストールする必要がある場合には、処理はブロック１５８に進む。そうでなく、スマート・チップのための登録データがすでにインストールされている場合には、処理はブロック１６４に進む。

【００４０】さらに図７を参照すると、ブロック１５８は、登録データとして記憶するための、ユーザ識別データのスマート・チップへのコピーを示す。その後、処理はブロック１５８からブロック１６２に進む。ブロック１６２は、スマート・コンパクト・ディスクの再生を示し、その後、処理はリターンする。

【００４１】さらに図７を参照すると、ブロック１６４は、スマート・カードからのユーザ識別データとスマート・チップからの登録データの比較を示す。その後、処理はブロック１６４からブロック１６６に進む。ブロック１６６は、ユーザ識別データがスマート・チップからの登録データと一致するか否かの判定を示す。データが一致する場合には、処理はブロック１６２に進む。データが一致しない場合には、処理はブロック１６８に進む。ブロック１６８は、正しい識別が供給されなかったのでエラー・メッセージが表示されることを示す。

【００４２】図７の処理は、データの許可されない複製から保護するだけではなく、スマート・コンパクト・ディスクを盗むことを阻止するためのセキュリティも提供する。たとえば、多くの店が、購入の前に顧客がコンパクト・ディスクに記憶された音楽を聞くことができるようにしている。しかし、コンパクト・ディスクのケーシングにセキュリティ保護が含まれないので、コンパクト・ディスクが簡単に盗まれる危険性がある。しかし、店内のスマート・コンパクト・ディスクのコピーがその店に登録され、スマート・コンパクト・ディスクを再生するための機械のすべてに、スマート・カードを用いてユーザ識別データが組み込まれている場合には、そのスマート・コンパクト・ディスクは、店内では再生できるが、そこから取り外された場合には役に立たなくなる。

【００４３】ここで図８を参照すると、本発明の方法およびシステムによる、スマート・コンパクト・ディスク、具体的にはスマートＤＶＤディスクの所有権登録をインストールするための方法の高水準論理流れ図が示されている。図からわかるように、図８に示された処理は、ブロック１８０で開始され、その後、ブロック１８２に進む。マイクロプロセッサ３０の動作における複数のトリガが、ブロック１８０で開始される処理のトリガになる可能性がある。たとえば、スマート・コンパクト・ディスクの検出時に、この処理にトリガをかけることができる。

【００４４】ブロック１８２は、スマート・カードからのユーザ識別データの読取を示す。ブロック１８２の後に、処理はブロック１８４に進む。ブロック１８４は、スマート・コンパクト・ディスクに取り付けられたスマート・チップからの登録データの読取を示す。その後、処理はブロック１８６に進む。ブロック１８６は、コンパクト・ディスクに添付されたスマート・チップに前に登録データがインストールされたか否かの判定を示す。スマート・チップのための登録データをインストールする必要がある場合には、処理はブロック１８８に進む。登録が前にインストールされている場合には、処理はブロック２００に進む。

【００４５】さらに図８を参照すると、ブロック１８８は、スマート・カードからの地理的ユーザ識別データと、スマート・コンパクト・ディスクに取り付けられたスマート・チップからの地理的登録データの比較を示す。スマート・チップには、スマート・コンパクト・ディスクの使用が意図された地理的地域が含まれる。その

後、処理はブロック１８８からブロック１９０に進む。ブロック１９０は、地理的データが一致するか否かの判定を示す。地理的データが一致する場合には、処理はブロック１９２に進む。しかし、地理的データが一致しない場合には、処理はブロック２０４に進む。ブロック２０４は、スマート・コンパクト・ディスクが地理的区域の外である場合のエラー・メッセージの表示を示す。ブロック１９２は、登録データとして記憶するための、ユーザ識別データのスマート・チップへのコピーを表す。その後、処理はブロック１９２からブロック１９８に進む。ブロック１９８は、ＤＶＤの再生の開始を示し、その後、処理はリターンする。

【００４６】さらに図８を参照すると、ブロック２００は、スマート・カードからのユーザ識別データと、スマート・コンパクト・ディスクに取り付けられたスマート・チップからの登録データの比較を示す。その後、処理はブロック２０２に進む。ブロック２０２は、ユーザ識別データが登録データと一致するか否かの判定を示す。データが一致する場合には、処理はブロック１９８に進み、前に説明したように進行する。そうでない場合には、処理はブロック２０４に進み、前に説明したように進行する。

【００４７】ここで図９を参照すると、本発明の方法およびシステムによる、スマート・コンパクト・ディスクの所有権をアンインストールする方法の高水準論理流れ図が示されている。図からわかるように、図９に示された処理は、ブロック２１０で開始され、その後、ブロック２１２に進む。マイクロプロセッサ３０の動作における複数のトリガが、ブロック２１０で開始される処理のトリガになる可能性がある。たとえば、スマート・コンパクト・ディスクの所有権をアンインストールすることを求めるユーザ要求の検出時に、この処理にトリガをかけることができる。

【００４８】ブロック２１２は、スマート・カードからのユーザ識別データの読取を示す。ブロック２１２の後に、処理はブロック２１４に進む。ブロック２１４は、スマート・コンパクト・ディスクに取り付けられたスマート・チップからの登録データの読取を示す。その後、処理はブロック２１４からブロック２１６に進む。ブロック２１６は、スマート・コンパクト・ディスクに取り付けられたスマート・チップに前に登録データがインストールされたか否かの判定を示す。スマート・チップのための登録データをインストールする必要がある場合には、処理はブロック２１８に進む。ブロック２１８は、スマート・チップが前のソフトウェア・インストールの記録を有しないのでエラー・メッセージが表示されることを示す。スマート・チップのための登録データが前にインストールされている場合には、処理はブロック２２０に進む。

【００４９】さらに図９を参照すると、ブロック２２０は、スマート・カードからのユーザ識別データと、スマート・コンパクト・ディスクに取り付けられたスマート・チップからの登録データの比較を示す。その後、処理はブロック２２０からブロック２２２に進む。ブロック２２２は、ユーザ識別データが登録データと一致するか否かの判定を示す。データが一致する場合には、処理はブロック２２４に進む。しかし、データが一致しない場合には、処理はブロック２２６に進む。ブロック２２６は、正しい識別が供給されなかったのでエラー・メッセージが表示されることを示す。

【００５０】さらに図９を参照すると、ブロック２２４は、スマート・チップからの登録データの消去を示す。登録データのアンインストール処理は、消費者が、コンパクト・ディスク、具体的にはオーディオＣＤまたはＤＶＤの所有権を別の個人に譲渡できるようにするために含まれる。ＤＶＤスマート・チップには、レンタル目的のＤＶＤを見ることができる回数を制御するためのカウンタも含めることができる。アンインストール処理中に、このカウンタはリセットされる。

【００５１】好ましい実施例に関して本発明を具体的に図示し、説明してきたが、本発明の趣旨および範囲から逸脱せずに、形態および詳細のさまざまな変更を行うことができることを、当業者は理解するであろう。たとえば、本発明の処理では、ユーザ識別データが、スマート・カードまたはハードウェアに組み込まれたスマート・カード・チップから取得される。しかし、他の実施態様では、すでに説明したように、ユーザ識別データを、データ処理システムに組み込まれたユーザ識別データなどの他の供給源から得ることができる。さらに、ユーザ識別データは、生物測定データを含むがこれに制限されない他の供給源から得ることができ、生物測定データの場合、コンパクト・ディスクへのアクセス権を得るために、コンパクト・ディスク所有者は、眼球スキャンまたは他の生物測定データ収集方法を介して自分自身を識別しなければならず、この場合、ユーザ識別データは、コンパクト・ディスクに添付されたスマート・チップに記憶される。

【００５２】さらに、たとえば、コンパクト・ディスクなどの光学的に認識可能なデータを含むデータ記憶媒体の利用に焦点を合わせて本発明を説明してきたが、本発明の趣旨から逸脱せずに、他の光学記憶装置で本発明の方法およびシステムを使用することもできる。さらに、スマート・チップの代わりに、他の電子記憶装置を使用することができる。

【００５３】さらに、たとえば、本発明の方法を指示するソフトウェアを実行するデータ記憶システムに関して本発明の諸態様を説明してきたが、本発明は、その代わりに、データ処理システムと共に使用するためのコンピュータ・プログラム製品として実施することができることを理解されたい。本発明の機能を定義するプログラム

は、非書込可能記憶媒体（たとえばCD－ROM）、書込可能記憶媒体（たとえばフロッピ・ディスケットまたはハード・ディスク装置）および、イーサネットを含むコンピュータ・ネットワークおよび電話ネットワークなどの通信媒体を含むがこれに制限されない、さまざまな信号担持媒体を介してデータ処理システムに配布することができる。したがって、そのような信号担持媒体は、本発明の方法機能を指示するコンピュータ可読命令を担持するか符号化する時に、本発明の代替実施例を表すことを理解されたい。

【００５４】まとめとして、本発明の構成に関して以下の事項を開示する。

【００５５】（１）基板と、前記基板が光学読取装置によって操作される時に読み取られるようになされた、前記基板内に組み込まれた光学的に認識可能なデータと、２つの別個のセキュリティ分類のデータを同一のデータ記憶装置に記憶できるように、電子的に変更可能なデータを記憶するための、前記基板に取り付けられた電子記憶装置とを含む、データ記憶装置。

（２）前記基板が、コンパクト・ディスクである、上記（１）に記載のデータ記憶装置。

（３）前記光学読取装置が、コンパクト・ディスク読取装置である、上記（１）に記載のデータ記憶装置。

（４）前記電子記憶装置が、スマート・チップである、上記（１）に記載のデータ記憶装置。

（５）さらに、前記基板に取り付けられた、前記電子記憶装置に対する加重バランスを含む、上記（１）に記載のデータ記憶装置。

（６）データ記憶装置内に組み込まれた光学的に認識可能なデータへのアクセスを保護する方法であって、データ記憶装置が読取装置に挿入されることに応答して、前記データ記憶装置に添付された電子記憶装置に登録データが記憶されているかどうかを判定するステップと、前記登録データをユーザ識別データと比較するステップと、データ記憶装置上の光学的に認識可能なデータへのアクセスが、正しい識別によってのみ許可されるように、前記登録データが前記ユーザ識別データと一致することに応答して、前記データ記憶装置内に組み込まれた前記光学的に認識可能なデータを読み取るステップとを含む方法。

（７）さらに、前記データ記憶装置上の前記光学的に認識可能なデータに対して行われるアクセスの数を追跡するために、前記光学的に認識可能なデータがアクセスされる時に、前記電子記憶装置に記憶された登録データを更新するステップを含む、上記（６）に記載のデータ記憶装置に記憶された光学的に認識可能なデータへのアクセスを保護する方法。

（８）さらに、前記光学的に認識可能なデータへの定義済みの量のアクセスが行われた後に、前記光学的に認識可能なデータへのアクセスを制限するステップを含む、上記（７）に記載のデータ記憶装置に記憶された光学的に認識可能なデータへのアクセスを保護する方法。

（９）さらに、前記データ記憶装置に添付された前記電子記憶装置に登録データが記憶されていない場合に、前記電子記憶装置に登録データを記憶するステップを含む、上記（６）に記載のデータ記憶装置に記憶された光学的に認識可能なデータへのアクセスを保護する方法。

（１０）前記データ記憶装置に添付された前記電子記憶装置に登録データが記憶されていない場合に、前記電子記憶装置に登録データを記憶する前記ステップが、さらに、前記ユーザ識別データにアクセスするステップと、前記電子記憶装置での記憶のための登録データとして前記ユーザ識別データを使用するステップとを含む、上記（９）に記載のデータ記憶装置に記憶された光学的に認識可能なデータへのアクセスを保護する方法。

（１１）前記ユーザ識別データにアクセスする前記ステップが、さらに、スマート・カードを検出するステップと、前記スマート・カードからの前記ユーザ識別データにアクセスするステップとを含む、上記（１０）に記載のデータ記憶装置に記憶された光学的に認識可能なデータへのアクセスを保護する方法。

（１２）前記データ記憶装置に添付された前記電子記憶装置に登録データが記憶されていない場合に、前記電子記憶装置に登録データを記憶する前記ステップが、さらに、前記ユーザ識別データ内に含まれる特定の地理的地域を、前記電子記憶装置に記憶された所定の地理的地域と比較するステップと、前記ユーザ識別データに含まれる前記特定の地理的地域が、前記電子記憶装置に記憶された前記所定の地理的地域と一致することに応答して、前記電子記憶装置での登録データの記憶を許可するステップとを含む、上記（９）に記載のデータ記憶装置に記憶された光学的に認識可能なデータへのアクセスを保護する方法。

（１３）前記登録データをユーザ識別データと比較する前記ステップが、さらに、前記ユーザ識別データにアクセスするステップを含む、上記（６）に記載のデータ記憶装置に記憶された光学的に認識可能なデータへのアクセスを保護する方法。

（１４）前記ユーザ識別データにアクセスする前記ステップが、さらに、スマート・カードを検出するステップと、前記スマート・カードからの前記ユーザ識別データにアクセスするステップとを含む、上記（１３）に記載のデータ記憶装置に記憶された光学的に認識可能なデータへのアクセスを保護する方法。

（１５）前記ユーザ識別データにアクセスする前記ステップが、さらに、前記読取装置に関連する、前記ユーザ識別データを記憶するスマート・チップを検出するステップと、前記検出されたスマート・チップから前記ユーザ識別データを読み取るステップとを含む、上記（１３）に記載のデータ記憶装置に記憶された光学的に認識

可能なデータへのアクセスを保護する方法。

（16）前記ユーザ識別データにアクセスする前記ステップが、さらに、前記読取装置を制御するオペレーティング・システムのインストール中に収集されたユーザ・データから前記ユーザ識別データを得るステップを含む、上記（13）に記載のデータ記憶装置に記憶された光学的に認識可能なデータへのアクセスを保護する方法。

（17）さらに、前記電子記憶装置上の前記登録データを変更するステップを含む、上記（6）に記載のデータ記憶装置に記憶された光学的に認識可能なデータへのアクセスを保護する方法。

（18）前記電子記憶装置上の前記登録データを変更する前記ステップが、さらに、前記光学的に認識可能なデータのすべてのコピーをアンインストールするステップと、前記電子記憶装置から前記登録データを消去するステップとを含む、上記（17）に記載のデータ記憶装置に記憶された光学的に認識可能なデータへのアクセスを保護する方法。

（19）データ記憶装置内に組み込まれた光学的に認識可能なデータへのアクセスを保護するためのシステムであって、データ記憶装置が読取装置に挿入されることに応答して、前記データ記憶装置に添付された電子記憶装置に登録データが記憶されているかどうかを判定するための手段と、前記登録データをユーザ識別データと比較するための手段と、データ記憶装置上の光学的に認識可能なデータへのアクセスが、正しい識別によってのみ許可されるように、前記登録データが前記ユーザ識別データと一致することに応答して、前記データ記憶装置内に組み込まれた前記光学的に認識可能なデータを読み取るための手段とを含むシステム。

（20）さらに、前記データ記憶装置上の前記光学的に認識可能なデータに対して行われるアクセスの数を追跡するために、前記光学的に認識可能なデータがアクセスされる時に、前記電子記憶装置に記憶された登録データを更新するための手段を含む、上記（19）に記載のデータ記憶装置に記憶された光学的に認識可能なデータへのアクセスを保護するためのシステム。

（21）さらに、前記光学的に認識可能なデータへの定義済みの量のアクセスが行われた後に、前記光学的に認識可能なデータへのアクセスを制限するための手段を含む、上記（20）に記載のデータ記憶装置に記憶された光学的に認識可能なデータへのアクセスを保護するためのシステム。

（22）さらに、前記データ記憶装置に添付された前記電子記憶装置に登録データが記憶されていない場合に、前記電子記憶装置に登録データを記憶するための手段を含む、上記（19）に記載のデータ記憶装置に記憶された光学的に認識可能なデータへのアクセスを保護するためのシステム。

（23）前記データ記憶装置に添付された前記電子記憶装置に登録データが記憶されていない場合に、前記電子記憶装置に登録データを記憶するための前記手段が、さらに、前記ユーザ識別データにアクセスするための手段と、前記電子記憶装置での記憶のための登録データとして前記ユーザ識別データを使用するための手段とを含む、上記（22）に記載のデータ記憶装置に記憶された光学的に認識可能なデータへのアクセスを保護するためのシステム。

（24）前記ユーザ識別データにアクセスするための前記手段が、さらに、スマート・カードからの前記ユーザ識別データにアクセスするためのスマート・カード読取装置を含む、上記（23）に記載のデータ記憶装置に記憶された光学的に認識可能なデータへのアクセスを保護するためのシステム。

（25）前記データ記憶装置に添付された前記電子記憶装置に登録データが記憶されていない場合に、前記電子記憶装置に登録データを記憶するための前記手段が、さらに、前記ユーザ識別データ内に含まれる特定の地理的地域を、前記電子記憶装置に記憶された所定の地理的地域と比較するための手段と、前記ユーザ識別データ内に含まれる前記特定の地理的地域が、前記電子記憶装置に記憶された前記所定の地理的地域と一致することに応答して、前記電子記憶装置での前記登録データの記憶を許可するための手段とを含む、上記（22）に記載のデータ記憶装置に記憶された光学的に認識可能なデータへのアクセスを保護するためのシステム。

（26）前記登録データをユーザ識別データと比較するための前記手段が、さらに、前記ユーザ識別データにアクセスするための手段を含む、上記（19）に記載のデータ記憶装置に記憶された光学的に認識可能なデータへのアクセスを保護するためのシステム。

（27）前記ユーザ識別データにアクセスする前記手段が、さらに、スマート・カードからの前記ユーザ識別データにアクセスするためのスマート・カード読取装置を含む、上記（26）に記載のデータ記憶装置に記憶された光学的に認識可能なデータへのアクセスを保護するためのシステム。

（28）前記ユーザ識別データにアクセスするための前記手段が、さらに、前記読取装置に関連する、前記ユーザ識別データを記憶するスマート・チップを検出するための手段と、前記検出されたスマート・チップから前記ユーザ識別データを読み取るための手段とを含む、上記（26）に記載のデータ記憶装置に記憶された光学的に認識可能なデータへのアクセスを保護するためのシステム。

（29）前記ユーザ識別データにアクセスするための前記手段が、さらに、前記読取装置を制御するオペレーティング・システムのインストール中に収集されたユーザ・データから前記ユーザ識別データを得るための手段を

含む、上記（２６）に記載のデータ記憶装置に記憶された光学的に認識可能なデータへのアクセスを保護するためのシステム。

（３０）さらに、前記電子記憶装置上の前記登録データを変更するための手段を含む、上記（１９）に記載のデータ記憶装置に記憶された光学的に認識可能なデータへのアクセスを保護するためのシステム。

（３１）前記電子記憶装置上の前記登録データを変更するための前記手段が、さらに、前記光学的に認識可能なデータのすべてのコピーをアンインストールするための手段と、前記電子記憶装置から前記登録データを消去するための手段とを含む、上記（３０）に記載のデータ記憶装置に記憶された光学的に認識可能なデータへのアクセスを保護するためのシステム。

（３２）データ記憶装置に組み込まれた光学的に認識可能なデータへのアクセスを保護するためのプログラム製品であって、データ処理システム使用可能媒体と、前記データ処理システム使用可能媒体を用いて符号化されたデータ記憶装置制御プログラムとを含み、前記データ記憶装置制御プログラムが、コンパクト・ディスク駆動装置へのコンパクト・ディスクの挿入に応答して、データ記憶装置に添付された電子記憶装置に登録データが記憶されているかどうかを判定し、前記登録データをユーザ識別データと比較し、データ記憶装置上の光学的に認識可能なデータへのアクセスが、正しい識別によってのみ許可されるように、前記登録データが前記ユーザ識別データと一致することに応答して、前記データ記憶装置内に組み込まれた前記光学的に認識可能なデータを読み取るプログラム製品。

（３３）前記データ記憶装置制御プログラムが、前記データ記憶装置上の前記光学的に認識可能なデータに対して行われるアクセスの数を追跡するために、前記光学的に認識可能なデータがアクセスされる時に、前記電子記憶装置に記憶された登録データを更新する、上記（３２）に記載のプログラム製品。

（３４）前記データ記憶装置制御プログラムが、前記光学的に認識可能なデータへの定義済みの量のアクセスが行われた後に、前記光学的に認識可能なデータへのアクセスを制限する、上記（３３）に記載のプログラム製品。

（３５）前記データ記憶装置制御プログラムが、前記データ記憶装置に添付された前記電子記憶装置に登録データが記憶されていない場合に、前記電子記憶装置に登録データを記憶する、上記（３２）に記載のプログラム製品。

（３６）前記データ記憶装置制御プログラムが、前記ユーザ識別データにアクセスし、前記電子記憶装置での記憶のための登録データとして前記ユーザ識別データを使用する、上記（３５）に記載のプログラム製品。

（３７）前記データ記憶装置制御プログラムが、スマート・カードからの前記ユーザ識別データにアクセスする、上記（３６）に記載のプログラム製品。

（３８）前記データ記憶装置制御プログラムが、前記ユーザ識別データ内に含まれる特定の地理的地域を、前記電子記憶装置に記憶された所定の地理的地域と比較し、前記ユーザ識別データに含まれる前記特定の地理的地域が、前記電子記憶装置に記憶された前記所定の地理的地域と一致することに応答して、前記電子記憶装置での登録データの記憶を許可する上記（３５）に記載のプログラム製品。

（３９）前記データ記憶装置制御プログラムが、前記ユーザ識別データにアクセスする、上記（３２）に記載のプログラム製品。

（４０）前記データ記憶装置制御プログラムが、スマート・カードからの前記ユーザ識別データにアクセスする、上記（３９）に記載のプログラム製品。

（４１）前記データ記憶装置制御プログラムが、前記読取装置に関連する、前記ユーザ識別データを記憶するスマート・チップを検出し、前記検出されたスマート・チップから前記ユーザ識別データを読み取る、上記（３９）に記載のプログラム製品。

（４２）前記データ記憶装置制御プログラムが、前記読取装置を制御するオペレーティング・システムのインストール中に収集されたユーザ・データから前記ユーザ識別データを得る、上記（３９）に記載のプログラム製品。

（４３）前記データ記憶装置制御プログラムが、前記電子記憶装置上の前記登録データを変更する、上記（３２）に記載のプログラム製品。

（４４）前記データ記憶装置制御プログラムが、前記光学的に認識可能なデータのすべてのコピーをアンインストールし、前記電子記憶装置から前記登録データを消去する、上記（４３）に記載のプログラム製品。

【図面の簡単な説明】

【図１】本発明の方法およびシステムによる、代表的なハードウェア環境を示す図である。

【図２】本発明の方法およびシステムによる、代表的なハードウェア環境の機能ブロック図である。

【図３】本発明の方法およびシステムによる、「スマート・カード」を高水準で表すブロック図である。

【図４】本発明の方法およびシステムによる、スマート・コンパクト・ディスクを高水準で表すブロック図である。

【図５】本発明の方法およびシステムによる、スマートＣＤ－ＲＯＭからのソフトウェアのインストールを許可するために、スマートＣＤ－ＲＯＭ上に登録データをインストールする方法の高水準論理流れ図である。

【図６】本発明の方法およびシステムによる、スマート・コンパクト・ディスクの所有権をアンインストールする方法の高水準論理流れ図である。

【図７】本発明の方法およびシステムによる、スマート・オーディオ・コンパクト・ディスク上のオーディオ・データにアクセスするために、スマート・オーディオ・コンパクト・ディスク上に登録データをインストールする方法の高水準論理流れ図である。

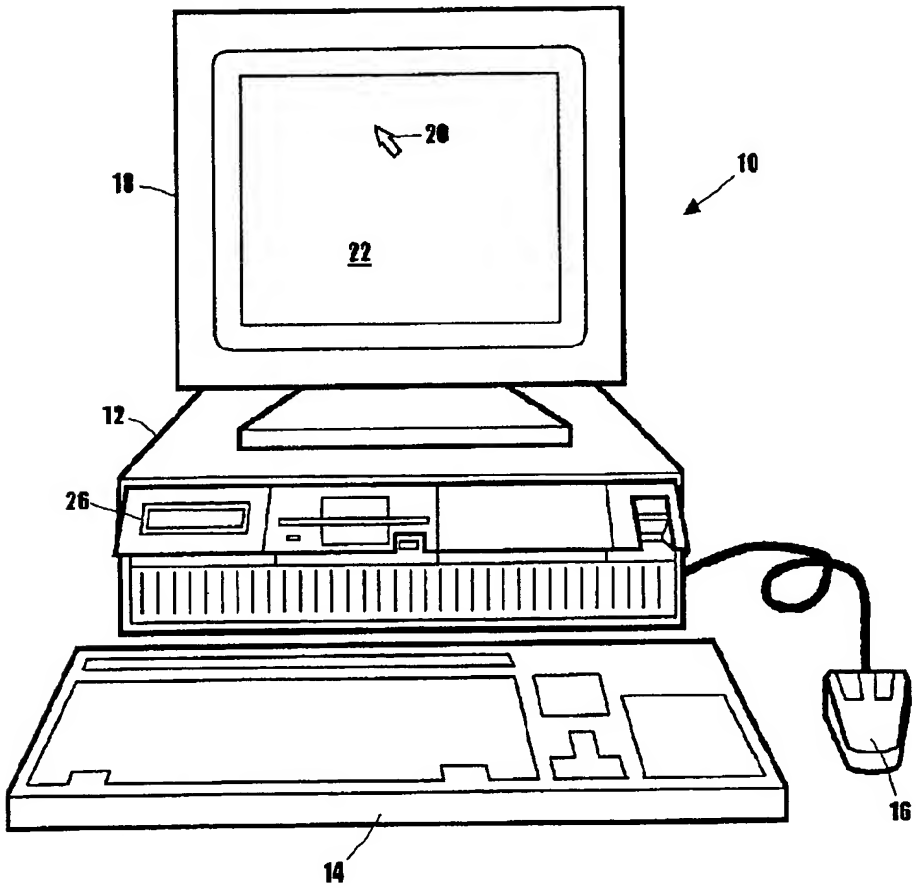
【図８】本発明の方法およびシステムによる、地理的位置に従ってスマートＤＶＤディスクに登録データをインストールする方法の高水準論理流れ図である。

【図９】本発明の方法およびシステムによる、スマートＤＶＤディスクの所有権をアンインストールする方法の高水準論理流れ図である。

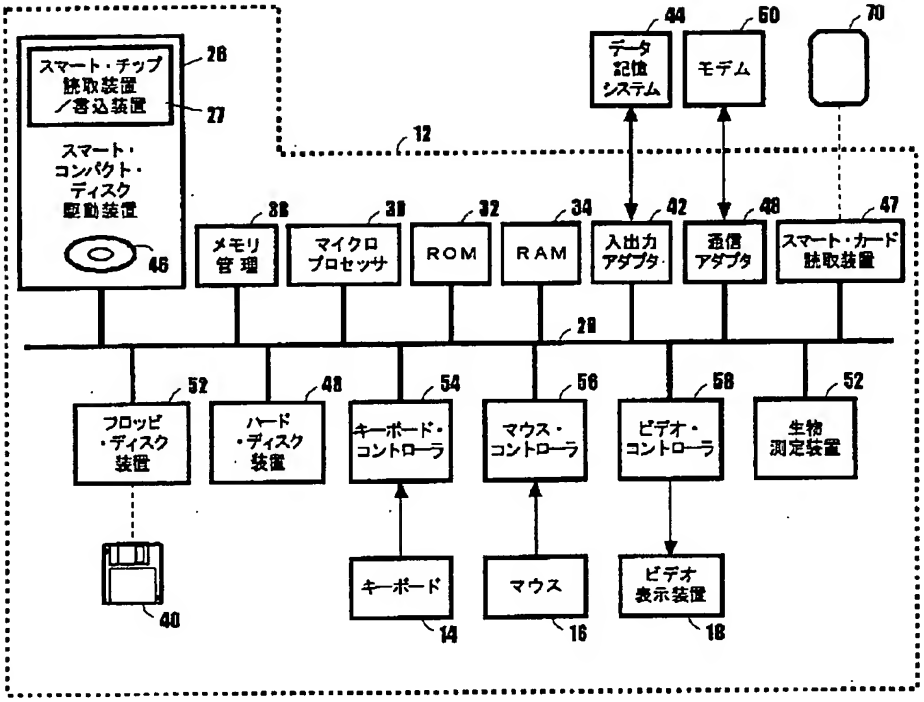
【符号の説明】

１２　プロセッサ・ユニット
２４　フロッピ・ディスク駆動装置
２６　スマート・コンパクト・ディスク駆動装置
２７　スマート・チップ読取装置／書込装置
２８　システム・バス
３０　マイクロプロセッサ
３２　読取専用メモリ（ＲＯＭ）
３４　ランダム・アクセス・メモリ（ＲＡＭ）
３６　ハード・ディスク装置
４２　入出力アダプタ
４４　データ記憶システム
４７　スマート・カード受入装置
４６　スマート・コンパクト・ディスク
５２　生物測定装置

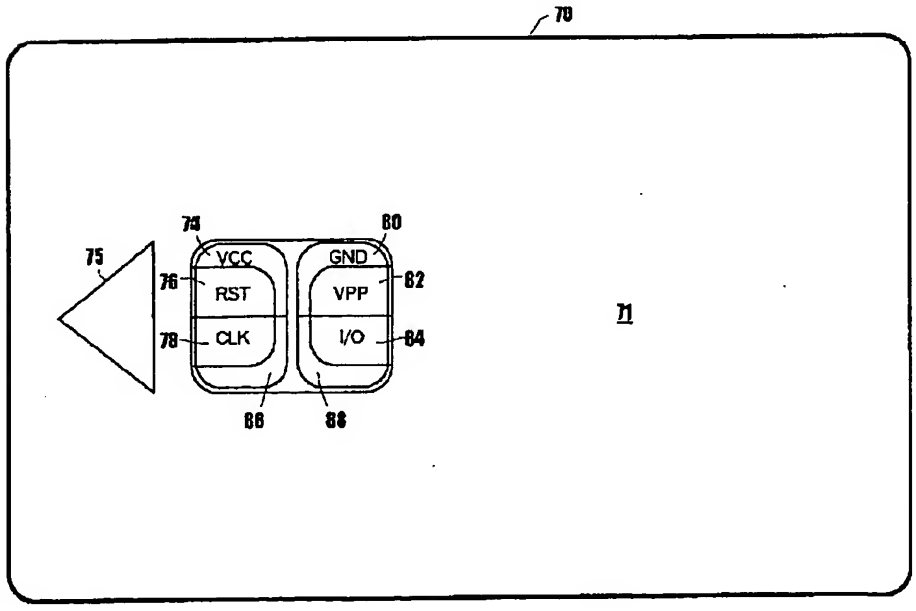
【図１】



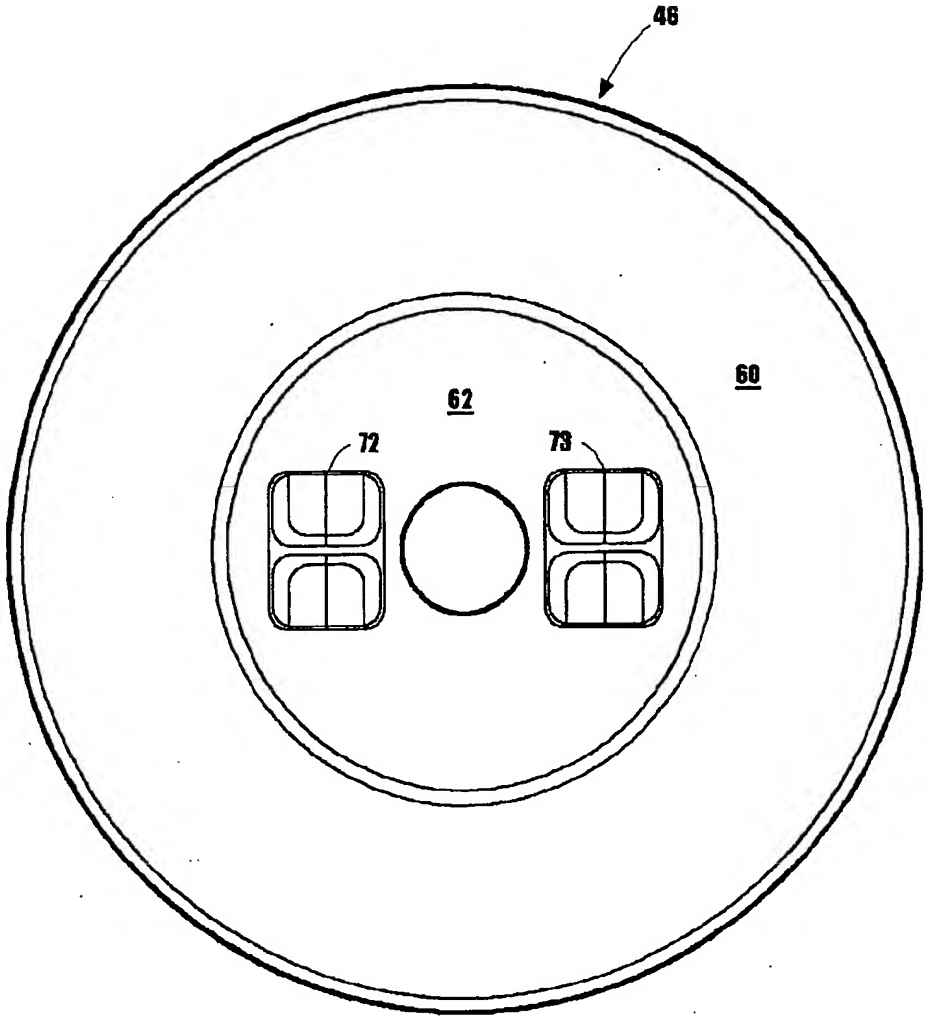
【図２】


スマート・チップ
読取装置
／書込装置
26
27
スマート・
コンパクト・
ディスク
駆動装置
46
12
44
データ
記憶
システム
60
モデム
70
メモリ
管理
38
マイクロ
プロセッサ
39
ROM
32
RAM
34
入出力
アダプタ
42
通信
アダプタ
48
スマート・カード
読取装置
47
28
フロッピ
・ディスク
装置
52
ハード
・ディスク
装置
48
キーボード・
コントローラ
54
マウス・
コントローラ
56
ビデオ・
コントローラ
58
生物
測定装置
52
40
キーボード
14
マウス
16
ビデオ
表示装置
18

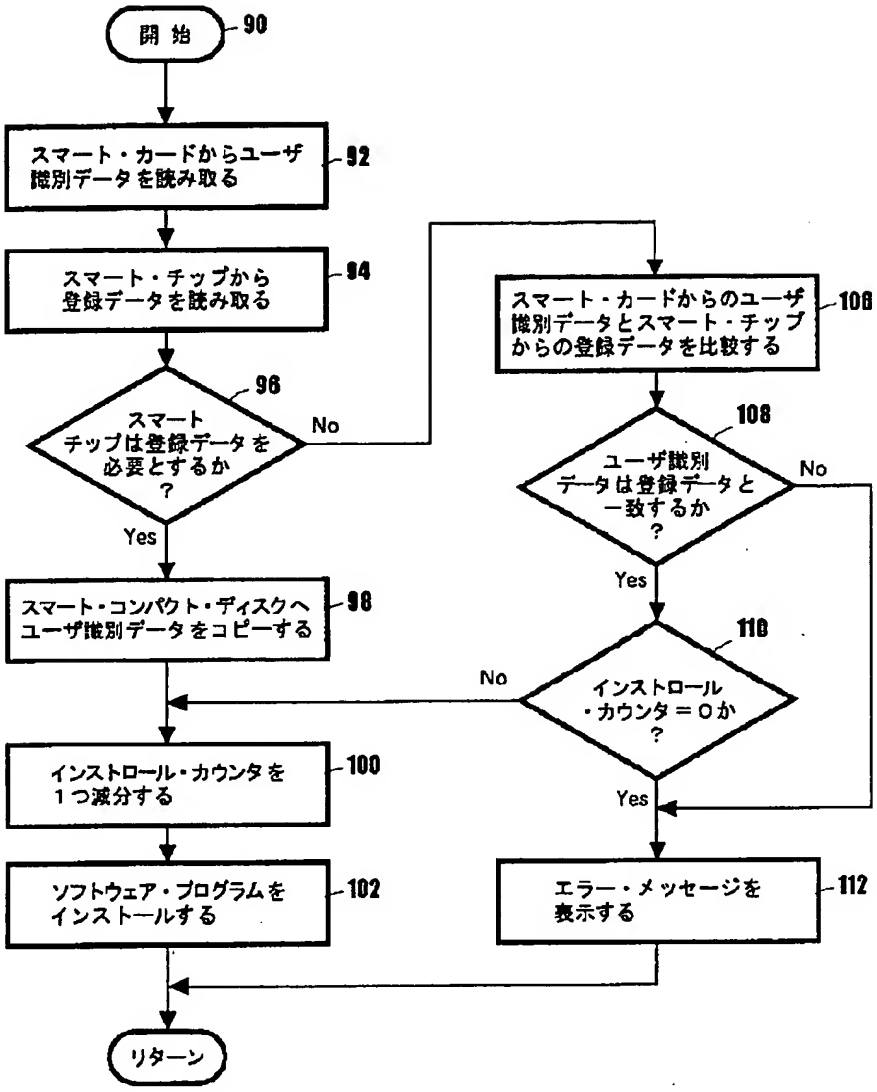
【図３】


70
75
74
VCC
80
GND
76
RST
82
VPP
78
CLK
84
I/O
86
86
71

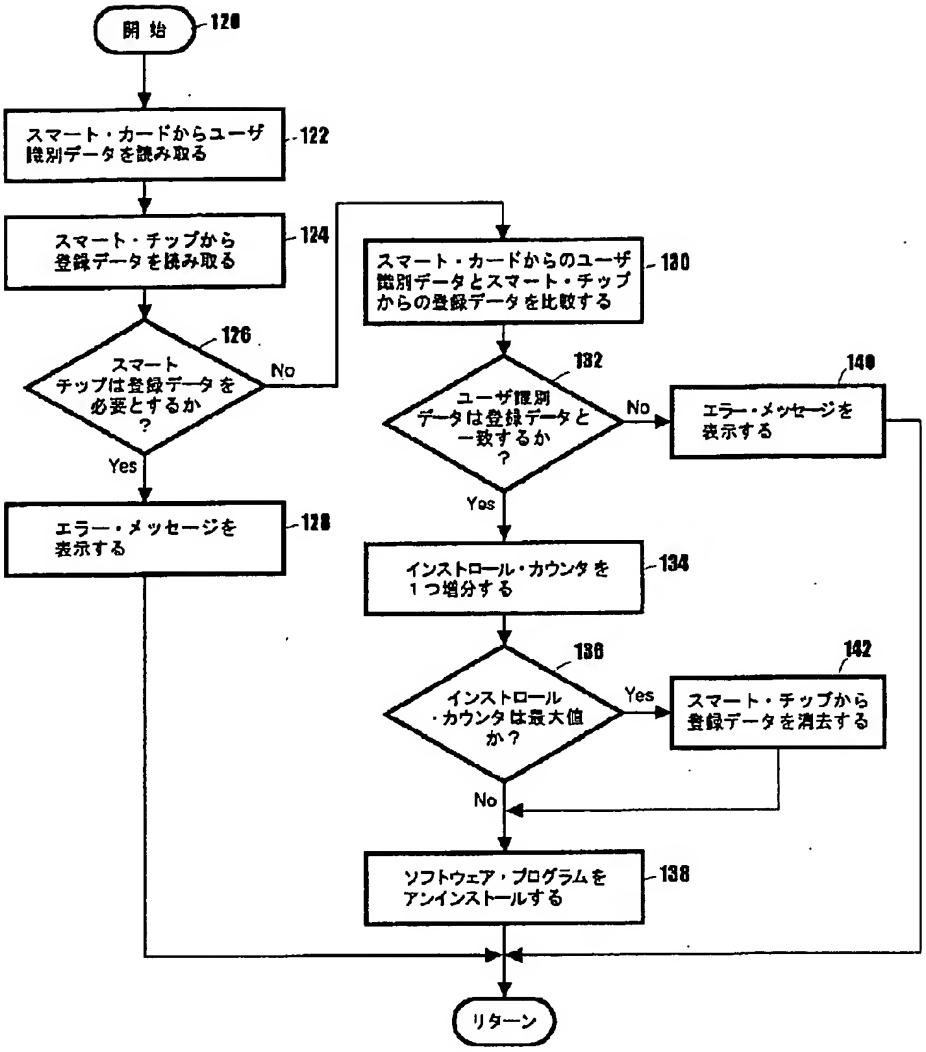
【図4】



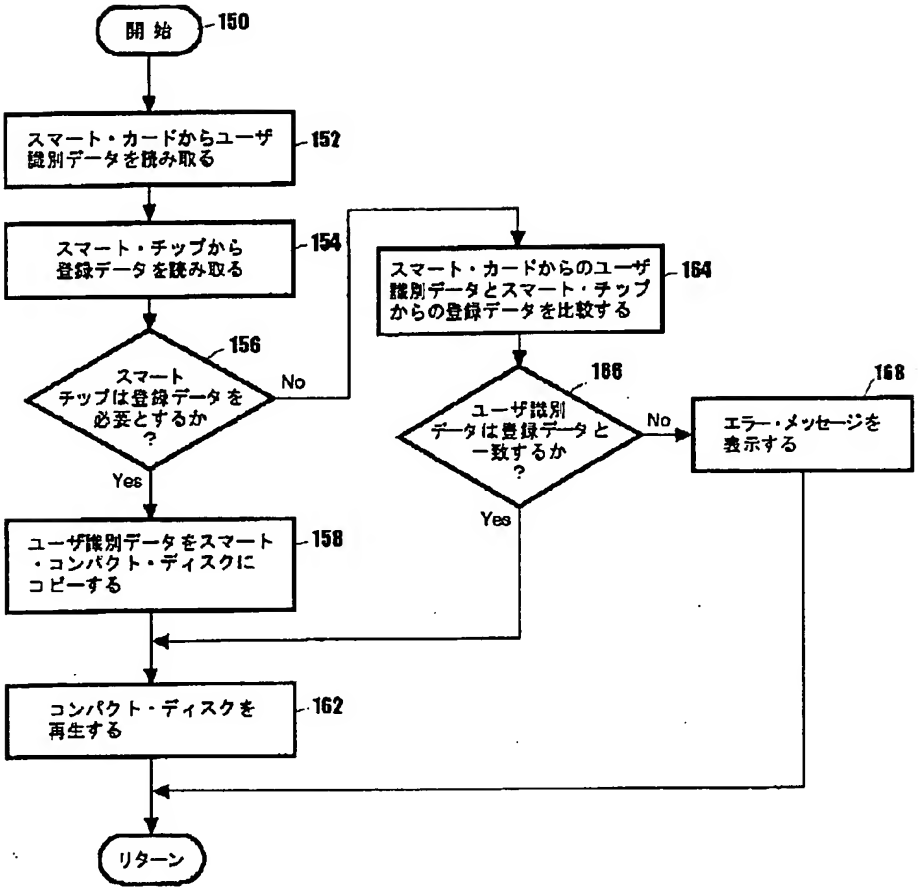
【図5】


開始
90
スマート・カードからユーザ識別データを読み取る
92
スマート・チップから登録データを読み取る
94
スマート・チップは登録データを必要とするか？
96
No
Yes
スマート・コンパクト・ディスクへユーザ識別データをコピーする
98
インストロール・カウンタを１つ減分する
100
ソフトウェア・プログラムをインストールする
102
リターン
スマート・カードからのユーザ識別データとスマート・チップからの登録データを比較する
106
ユーザ識別データは登録データと一致するか？
108
No
Yes
インストロール・カウンタ＝０か？
110
No
Yes
エラー・メッセージを表示する
112

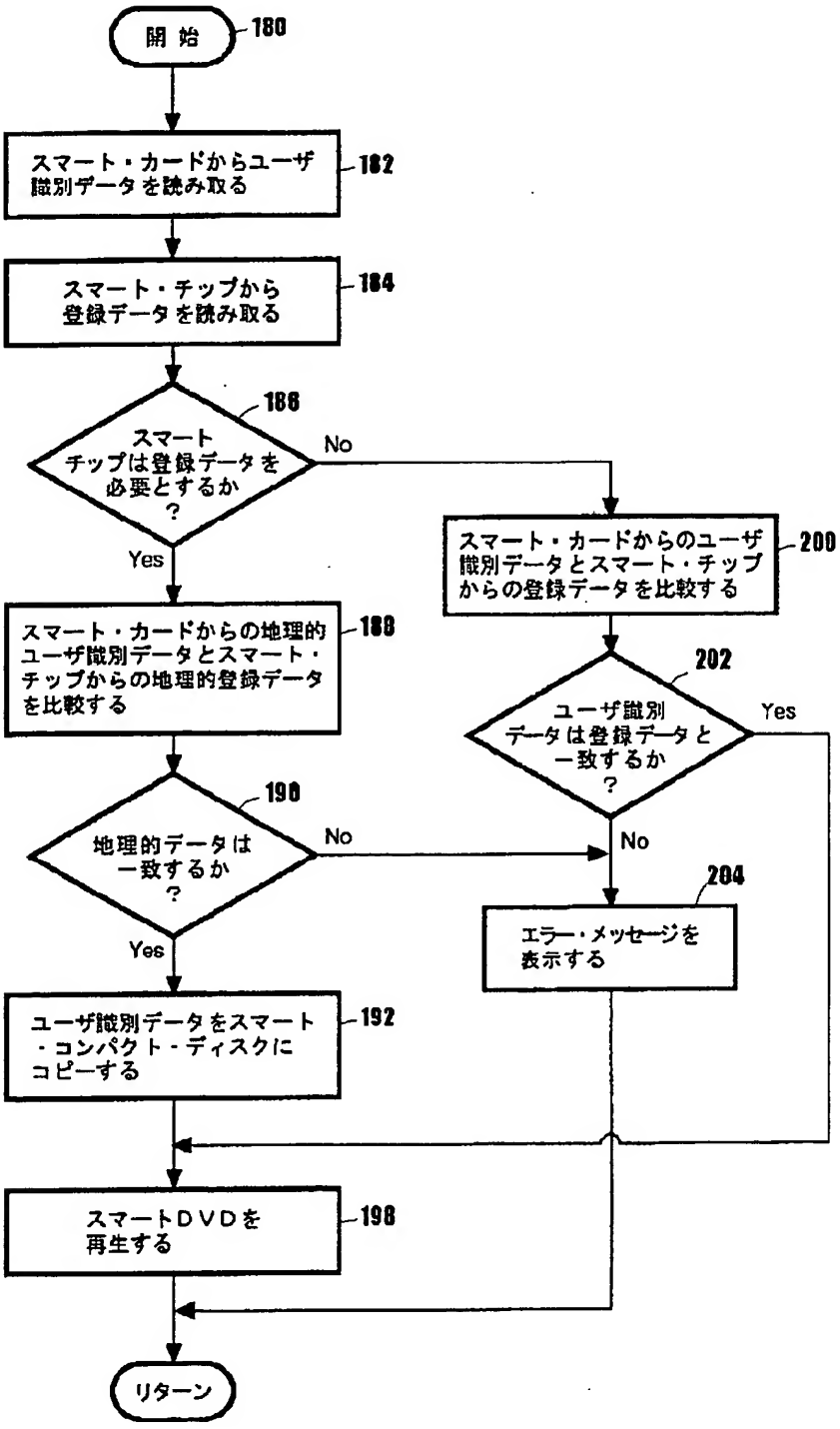
【図6】


開始
120
スマート・カードからユーザ識別データを読み取る
122
スマート・チップから登録データを読み取る
124
スマート・チップは登録データを必要とするか？
126
No
Yes
エラー・メッセージを表示する
128
スマート・カードからのユーザ識別データとスマート・チップからの登録データを比較する
130
ユーザ識別データは登録データと一致するか？
132
No
エラー・メッセージを表示する
140
Yes
インストロール・カウンタを1つ増分する
134
インストロール・カウンタは最大値か？
136
Yes
スマート・チップから登録データを消去する
142
No
ソフトウェア・プログラムをアンインストールする
138
リターン

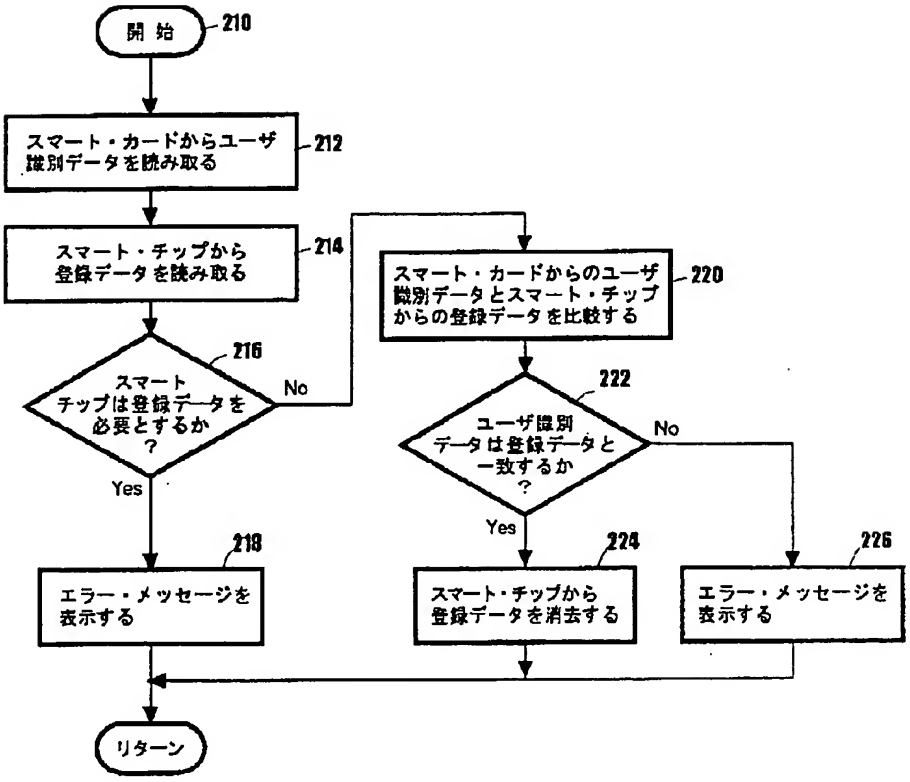
【図7】


開始
150
スマート・カードからユーザ識別データを読み取る
152
スマート・チップから登録データを読み取る
154
スマート・チップは登録データを必要とするか？
156
No
Yes
ユーザ識別データをスマート・コンパクト・ディスクにコピーする
158
コンパクト・ディスクを再生する
162
リターン
スマート・カードからのユーザ識別データとスマート・チップからの登録データを比較する
164
ユーザ識別データは登録データと一致するか？
166
No
Yes
エラー・メッセージを表示する
168

【図8】


開始
180
スマート・カードからユーザ識別データを読み取る
182
スマート・チップから登録データを読み取る
184
スマート・チップは登録データを必要とするか？
186
No
Yes
スマート・カードからのユーザ識別データとスマート・チップからの登録データを比較する
200
スマート・カードからの地理的ユーザ識別データとスマート・チップからの地理的登録データを比較する
188
ユーザ識別データは登録データと一致するか？
202
Yes
No
地理的データは一致するか？
190
No
Yes
エラー・メッセージを表示する
204
ユーザ識別データをスマート・コンパクト・ディスクにコピーする
192
スマートDVDを再生する
198
リターン

【図9】



フロントページの続き

(72)発明者 ポール・ロバート・ハバール
アメリカ合衆国78681 テキサス州ラウンド・ロック オークリッジ・ドライブ 1503

(72)発明者 ジョージ・コッコスリス
アメリカ合衆国78729 テキサス州オースチン ウィンドラッシュ・ドライブ 7701

(72)発明者 スチーブン・ジョーゼフ・スモルスキ
アメリカ合衆国78733 テキサス州オースチン ウッド・レーク・サークル 302